WEB APPLICATION FIREWALL

FortiWeb-VM for Azure Install Guide

VERSION 5.6

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

September 23, 2016

FortiWeb 5.6 Install Guide for Azure

1st Edition

TABLE OF CONTENTS

Overview of FortiWeb-VM for Azure **4**
- Benefits 4
- Architecture 5
- Licensing 6

System requirements **7**
Downloading the FortiWeb-VM license & registering with Technical Support **8**
Deploying FortiWeb-VM for Azure **9**
Connecting to FortiWeb's web UI & CLI **17**
Uploading the license **18**
Integrating with Azure Event Hub **20**
What's next? **25**

Overview of FortiWeb-VM for Azure

Welcome, and thank you for selecting Fortinet products to protect your network.

FortiWeb-VM is a virtual appliance version of FortiWeb. FortiWeb-VM models are suitable for medium and large enterprises, as well as service providers.

Microsoft Azure is Microsoft's cloud computing platform and infrastructure. It allows you to build, deploy, and manage applications and services through a global network of data centers.

Benefits

FortiWeb is designed specifically to protect web servers.

FortiWeb web application firewalls (WAF) provide specialized application layer threat detection and protection for many HTTP or HTTPS services, including:

- Apache Tomcat
- nginx
- Microsoft IIS
- JBoss
- IBM Lotus Domino
- Microsoft SharePoint
- Microsoft Outlook Web App (OWA)
- RPC and ActiveSync for Microsoft Exchange Server
- Joomla
- WordPress

FortiWeb's integrated web vulnerability scanner can drastically reduces challenges associated with protecting regulated and confidential data by detecting your exposure to the latest threats, especially the OWASP Top 10.

In addition, FortiWeb's XML firewall and denial-of-service (DoS) attack-prevention protect your Internet-facing web-based applications from attack and data theft. Using advanced techniques to provide bidirectional protection against sophisticated threats like SQL injection and cross-site scripting (XSS), FortiWeb helps you prevent identity theft, financial fraud, and corporate espionage. FortiWeb delivers the technology you need to monitor and enforce government regulations, industry best practices, and internal security policies, including firewalling and patching requirements from PCI DSS.

FortiWeb's application-aware firewalling and load balancing engine can:

- Secure HTTP applications that are often gateways into valuable databases
- Prevent and reverse defacement
- Improve application stability
- Monitor servers for downtime & connection load
- Reduces response times
- Accelerate SSL/TLS *

- Accelerate compression/decompression
- Rewrite content on the fly

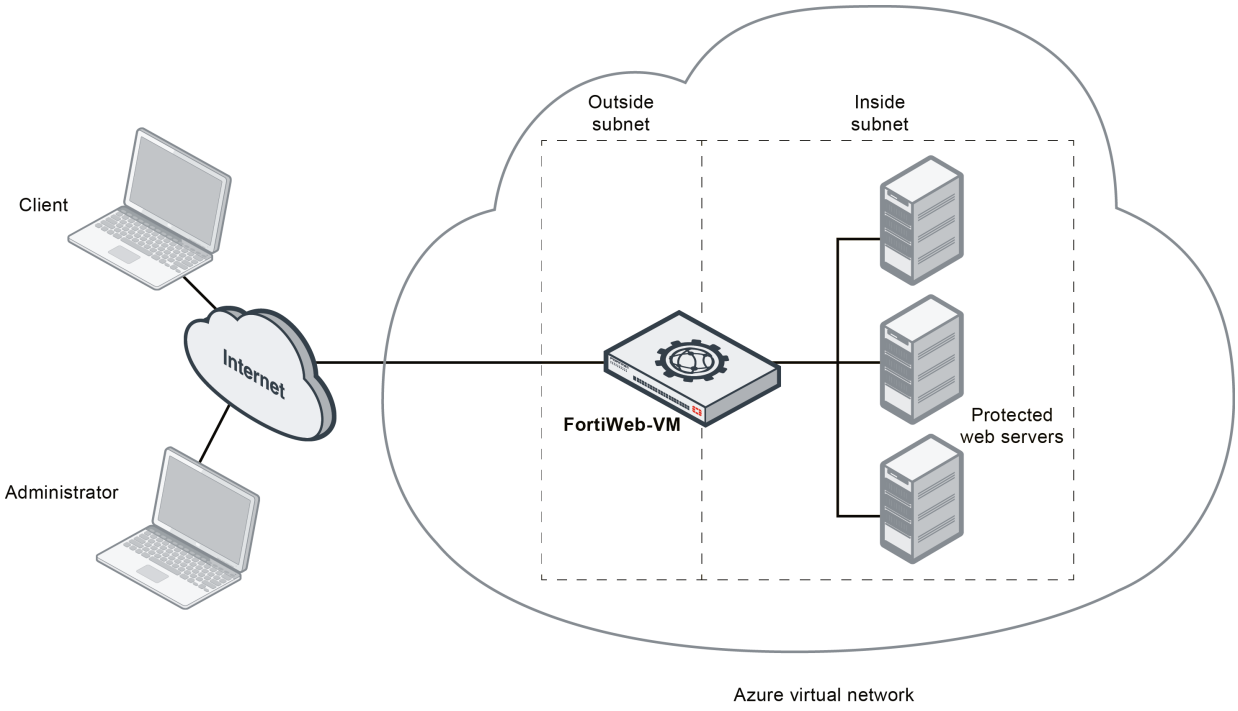
***** On VM models, acceleration is due to offloading the cryptography burden from the back-end server. On hardware models with ASIC chips, cryptography is also hardware-accelerated.

FortiWeb significantly reduces deployment costs by consolidating WAF, hardware acceleration, load balancing, and vulnerability scanning into a single device with no per-user pricing. Those features drastically reduce the time required to protect your regulated, Internet-facing data and eases the challenges associated with policy enforcement and regulatory compliance.

Architecture

You deploy FortiWeb-VM in the Microsoft Azure cloud platform as part of a virtual network.

FortiWeb-VM for Azure network topology



FortiWeb-VM for Azure operates in reverse proxy mode only. It is positioned inline to intercept all incoming client connections on the public subnet and scan and redistribute them to servers on the private subnet.

In a typical deployment, the FortiWeb outgoing interface connects to the Azure Public Load Balancer.

Once the virtual appliance is deployed, you can configure FortiWeb-VM via either its web UI (from a web browser) or CLI (from a terminal emulator).

Licensing

Azure deployments require FortiWeb-VM licenses that specify the size of the virtual appliance you can deploy. In addition, you use the registration number that you use to obtain the license to register for FortiGuard services and technical support.

No trial license is available for FortiWeb-VM for Azure.

FortiWeb-VM for Azure licenses are available for the following sizes of virtual machine:

FortiWeb-VM Compatible Azure Instances

License/model	Azure instance	vCPU	RAM	vNICs
FWB-VM02-AZ	D2	2	7 GB	2
	D2_v2	2	7 GB	2
FWB-VM04-AZ	A3	4	7 GB	2
	D3	4	14 GB	4
	D3_v2	4	14 GB	4
FWB-VM08-AZ	A4	8	14 GB	4
	D4	8	28 GB	8
	D4_v2	8	28 GB	8

The maximum number of IP sessions and policies an instance can support is determined by the license and available vRAM, just as it does for hardware models. For details, see maximum configuration values in the *FortiWeb Administration Guide*.

When you place an order for FortiWeb-VM, Fortinet emails a registration number to the recipient address you supplied on the order form. To register your appliance with Technical Support and to obtain a license file, enter that registration number on the Fortinet Technical Support web site at the following location:

https://support.fortinet.com/

For information on using the license file to activate FortiWeb-VM, see Downloading the FortiWeb-VM license & registering with Technical Support on page 8.

System requirements

To deploy FortiWeb-VM for Azure, first ensure you have the following resources:

- A Microsoft account, which allows you to log in to the Azure Preview Portal.
- An Azure subscription. You can subscribe during the deployment process and a trial subscription is available.
- A FortiWeb-VM license. See Licensing on page 6.
- Optionally, an Azure virtual network and storage account. The FortiWeb-VM deployment process allows you to create a new virtual network and storage account to use.

Downloading the FortiWeb-VM license & registering with Technical Support

When you purchase FortiWeb-VM from your reseller, you receive an email that contains a registration number. Use this number to download your license and register for technical support.

Many Fortinet customer services such as firmware updates, technical support, and FortiGuard services require product registration.

For more information, see Licensing on page 6 and the Fortinet Knowledge Base article Registration Frequently Asked Questions.

To register & download your FortiWeb-VM license

1. On your management computer, start a web browser.
2. Log in to the Fortinet Technical Support web site:

   https://support.fortinet.com/
3. In the **Asset Management** quadrant of the page, click **Register/Renew**.
4. Provide the registration number that was emailed to you when you purchased the software. Registration numbers are a hyphenated mixture of 25 numbers and characters in groups of 5. For example:

   `12C45-AB3DE-678G0-F9HIJ-123B5`

   A registration form is displayed.
5. Complete the form to register your ownership of FortiWeb-VM with Technical Support.

   After you complete the form, a registration acknowledgement page is displayed.
6. Click the **License File Download** link.

   Your browser downloads the `.lic` file that was purchased for that registration number.

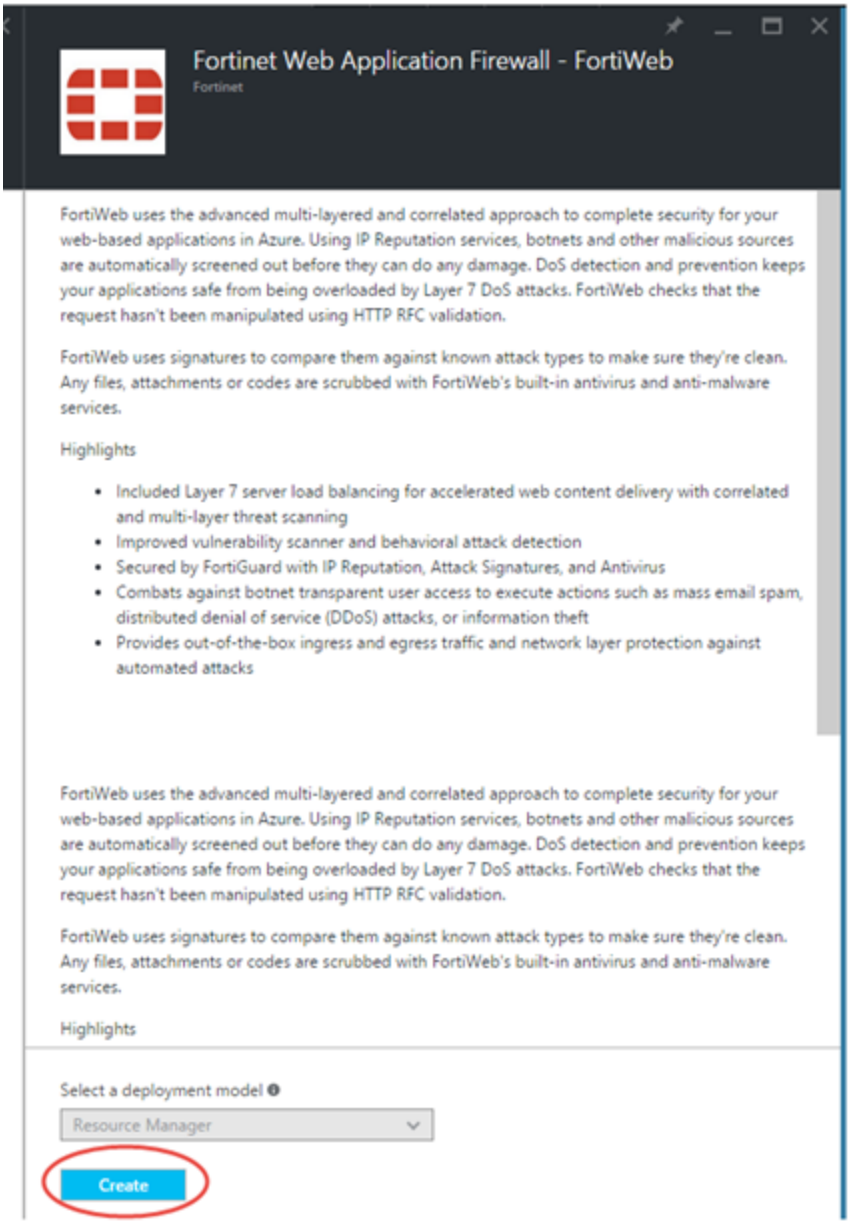
   You upload the license later, after you have deployed a FortiWeb instance in Azure.

Deploying FortiWeb-VM for Azure

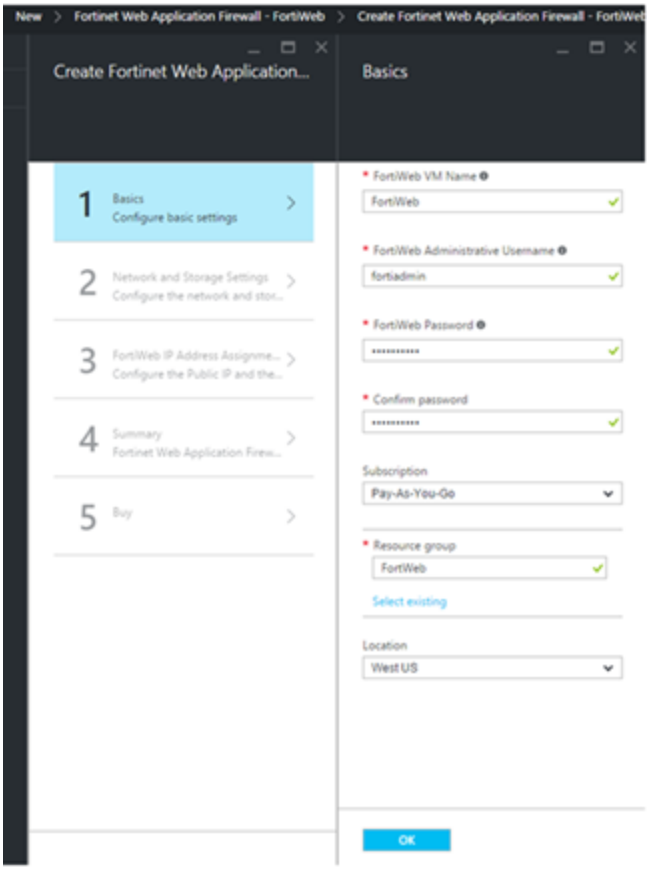
1. Log in to the Azure Preview Portal at the following location:

   https://portal.azure.com

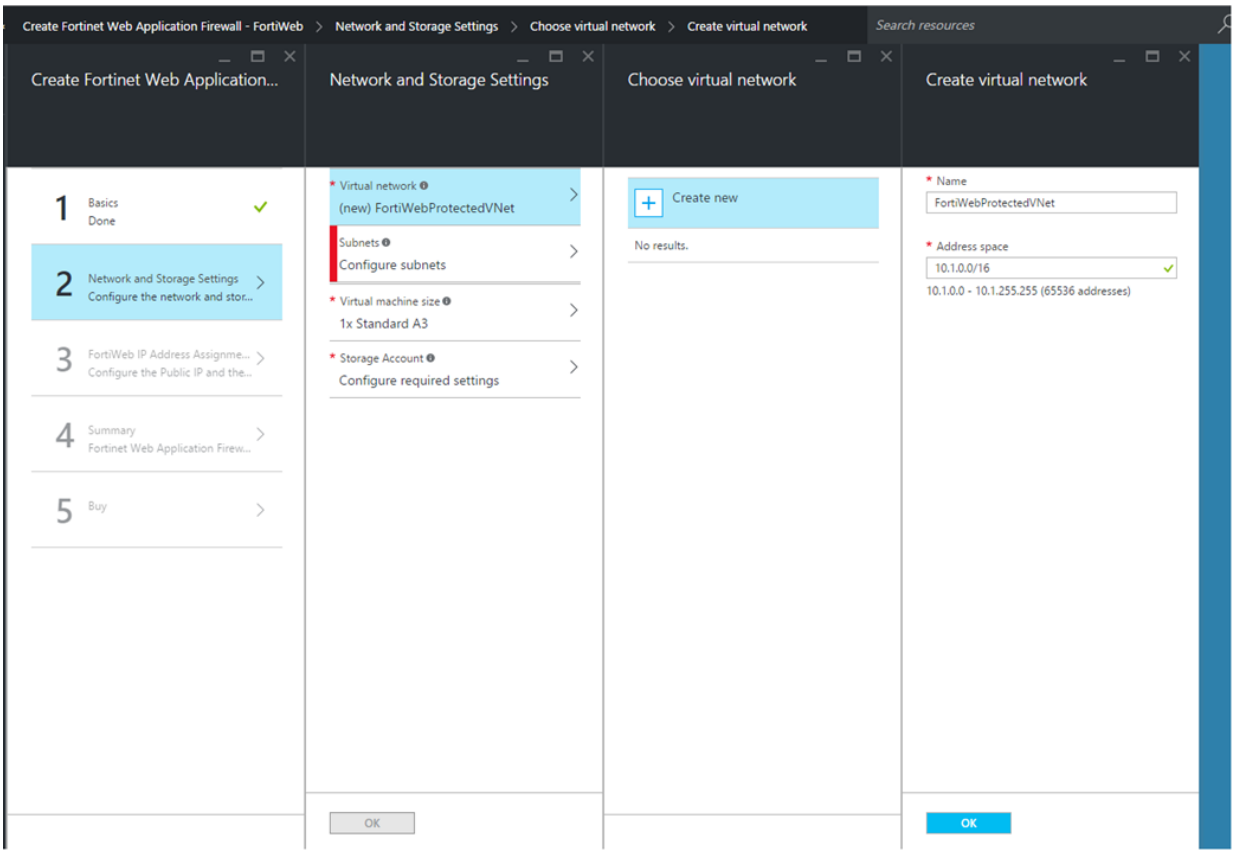
2. Click **New**, and then use the Marketplace search tool to locate and select FortiWeb.
3. Click **Create**.

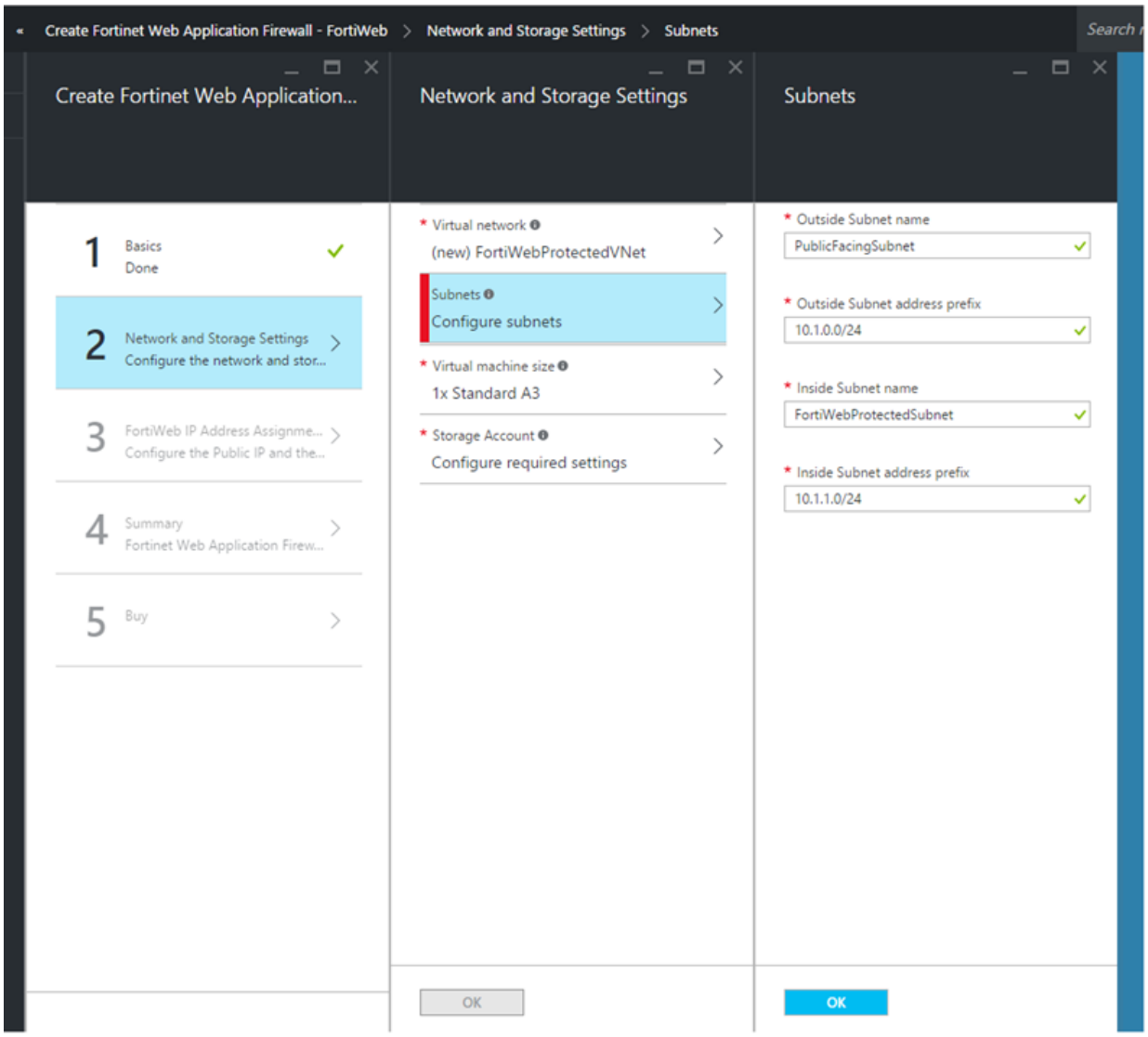


4. Complete the basic settings.



5. Under Network and Storage settings, select a virtual network or create a new one. Then, configure the subnets.


Create Fortinet Web Application Firewall - FortiWeb
Network and Storage Settings
Choose virtual network
Create virtual network
Search resources
Create Fortinet Web Application...
Network and Storage Settings
Choose virtual network
Create virtual network
1 Basics
Done
2 Network and Storage Settings
Configure the network and stor...
3 FortiWeb IP Address Assignme...
Configure the Public IP and the...
4 Summary
Fortinet Web Application Firew...
5 Buy
* Virtual network
(new) FortiWebProtectedVNet
Subnets
Configure subnets
* Virtual machine size
1x Standard A3
* Storage Account
Configure required settings
OK
Create new
No results.
* Name
FortiWebProtectedVNet
* Address space
10.1.0.0/16
10.1.0.0 - 10.1.255.255 (65536 addresses)
OK

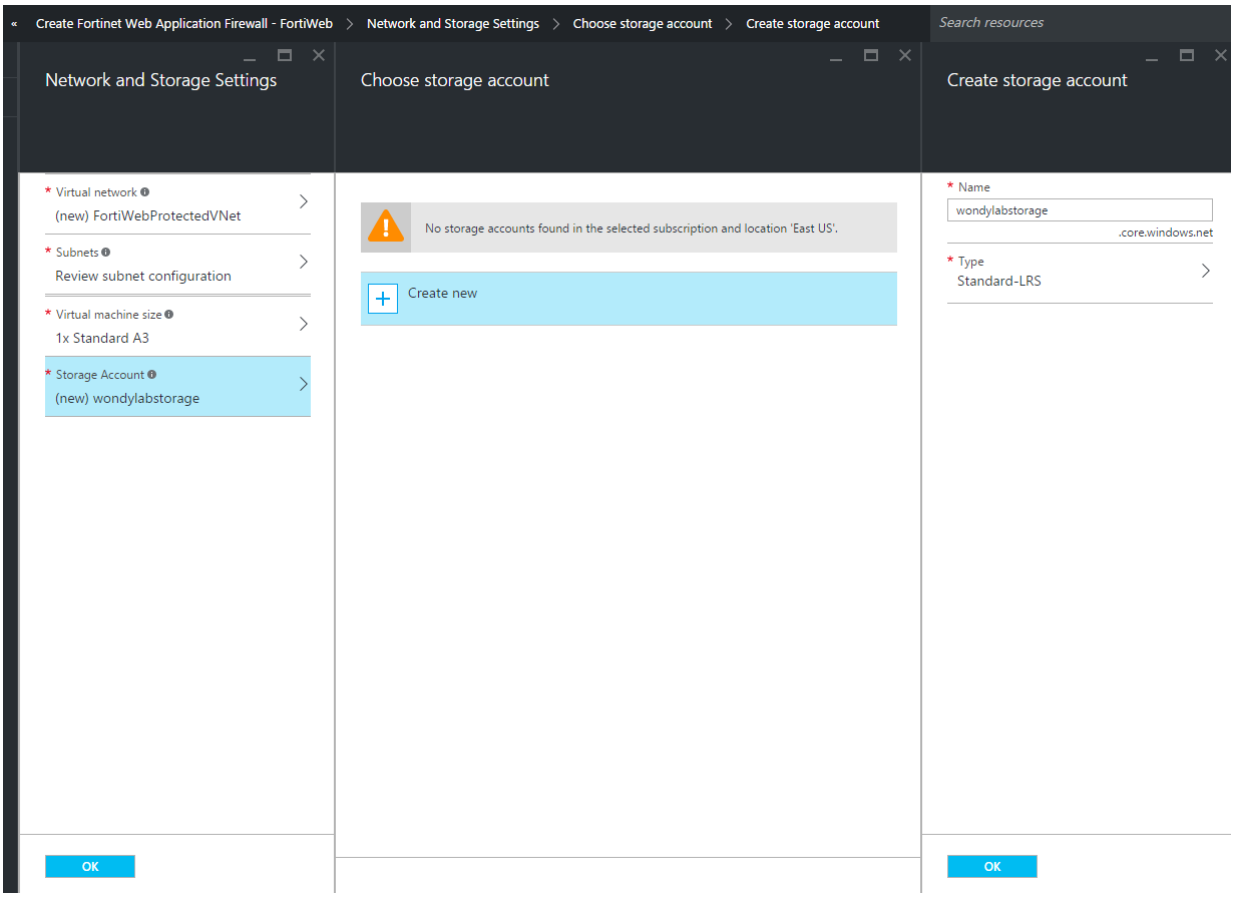


If you select an existing virtual network, ensure that is has at least two subnets for FortiWeb to route between: an "outside" or public subnet that provides access to the Internet and a private subnet where one or more servers that FortiWeb protects are located.

In a typical deployment, because the “outside” or public subnet simply connects the FortiWeb outgoing interface to the Azure Public Load Balancer, the subnet can be small.

6. Select the virtual machine size that is appropriate for your license. For more information, see Licensing on page 6.

7. For Storage Account, select an existing account or create a new one.

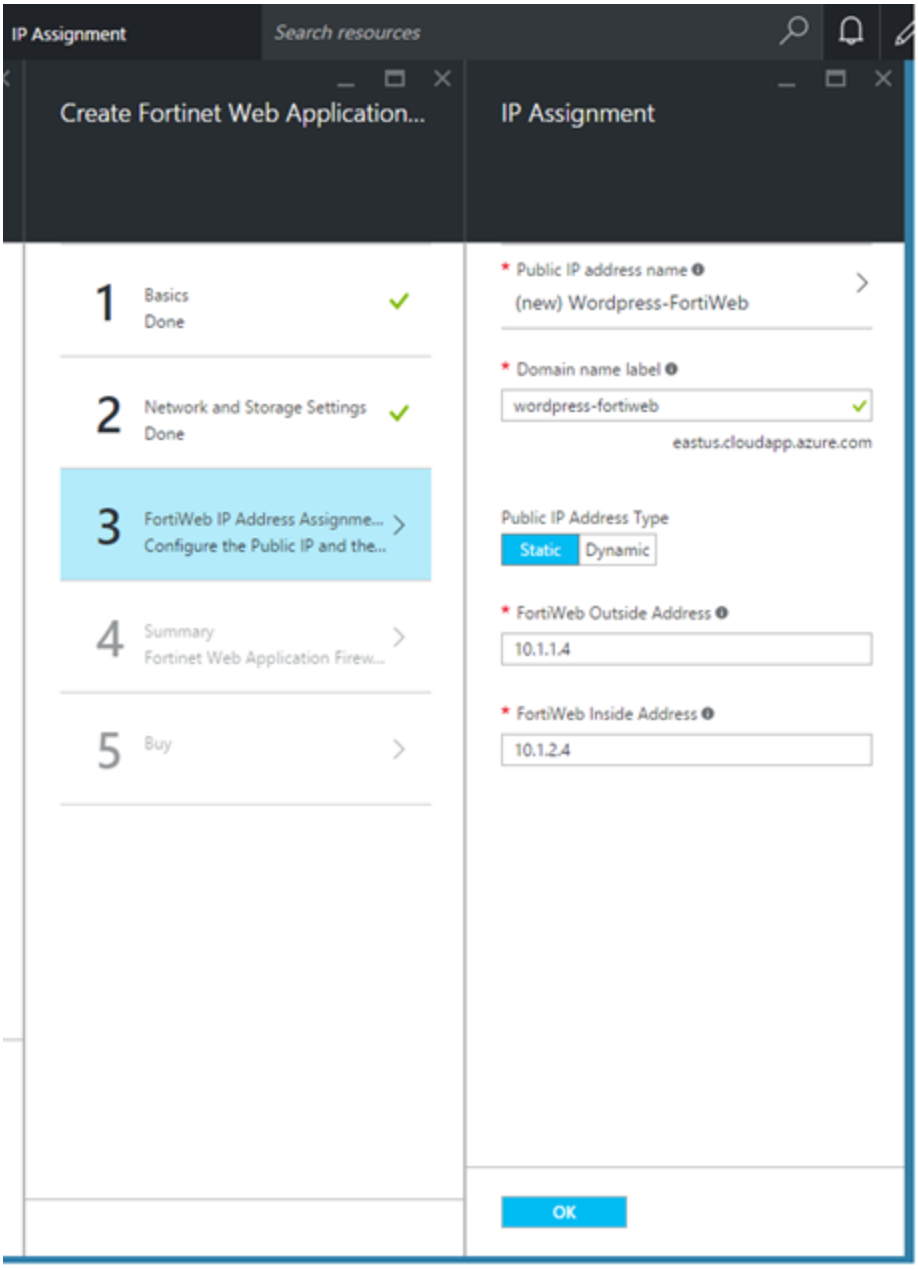


You cannot select a storage account in a location that is different than the one you selected in the basic settings.

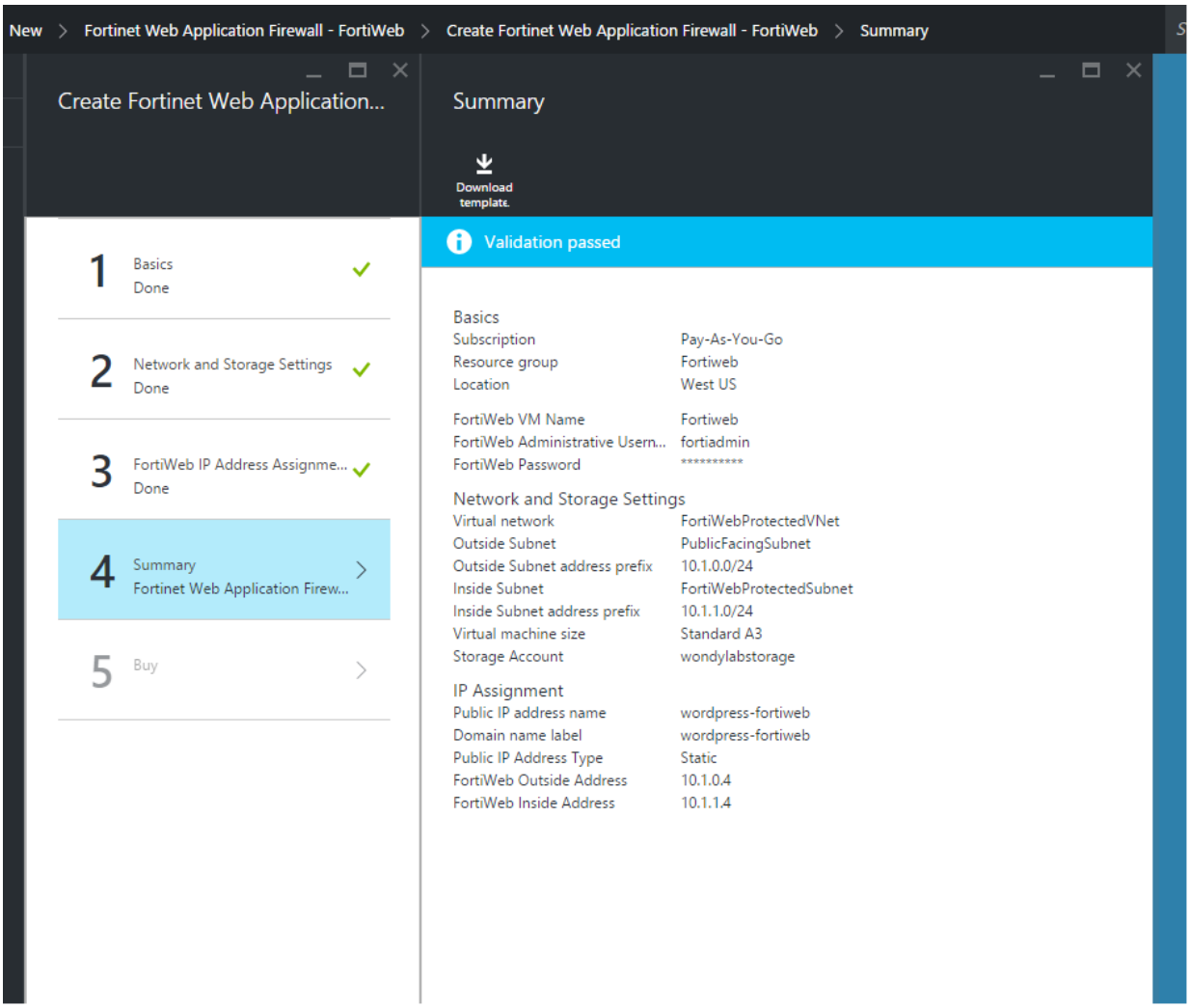
8. Configure the following IP settings:

Public IP Address name **Domain name label**	In a typical environment, the public IP address is the address of a load balancer that clients use to access your FortiWeb and the servers it protects from the Internet. In some cases, such as when you use ExpressRoute or an Azure VPN to access your virtual network, the appropriate setting is **none**.
Public IP Address Type	• **Static** – Azure preserves the public IP address after state changes such as restart and shutdown. • **Dynamic** – Azure assigns a new public IP address after state changes such as restart and shutdown.

FortiWeb Outside Address **FortiWeb Inside Address**	By default, for the outside and inside addresses, Azure selects the first useable address in the subnet (Azure uses the first three addresses in each subnet). However, when you deploy using an existing subnet, it is possible that other resources are already using these addresses. Because Azure cannot verify if the addresses are not used elsewhere, ensure that the IP addresses are available and in the correct subnet.



9. Navigate to the summary and review your deployment configuration.



10. Click **Purchase**.

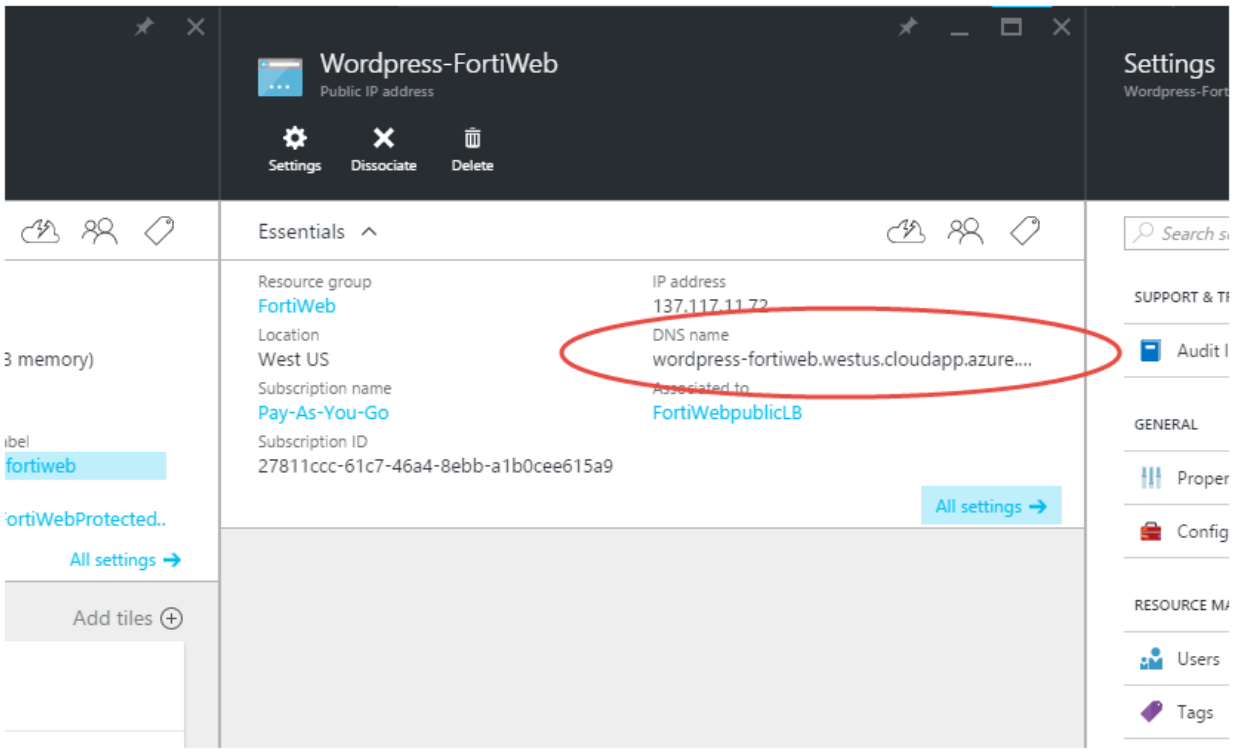
    This step purchases time on the Azure virtual machine, not the FortiWeb-VM license. You obtain the license to activate FortiWeb separately.

11. Wait for Azure to complete the deployment.

    In most cases, deployment takes about 20 minutes, but the amount of time varies depending on your location and the number of resources you requested.

    When the deployment is complete, all the resources the template provides are displayed.

12. To view your DNS name or public IP address, select the public IP resource.



13. Use the public IP address displayed in the Azure instance information to access the web UI in a web browser or the CLI using an SSH connection. See Connecting to FortiWeb's web UI & CLI on page 17.

Connecting to FortiWeb's web UI & CLI

After you deploy FortiWeb-VM for Azure, you use the public IP address displayed in the Azure instance information to access the web UI in a web browser or the CLI using an SSH connection.

To connect to the web UI

1. Enter the public IP address displayed in the Azure instance information in a web browser's address field.
2. Log in using the username and password you specified in the Azure virtual machine basic settings (**FortiWeb Administrative Username** and **FortiWeb Password**).

To connect to the CLI via SSH

These instructions connect to FortiWeb-VM for Azure using PuTTY terminal emulation software.

1. On your management computer, start PuTTY.
2. To ensure that your configuration does not use environment variables that can interfere with the connection, in the **Category** tree, expand **Connection**, and then click **Data.** Remove any environment variables.
3. Click **Session**, and for **Host Name (or IP Address)**, enter the public IP address of the FortiWeb-VM Azure instance.
4. In Port, type `22`.
5. For **Connection type**, select **SSH**.
6. Select **Open**.

   The SSH client connects to the FortiWeb appliance.

   The SSH client may display a warning if this is the first time you are connecting to the FortiWeb appliance and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiWeb appliance but it used a different IP address or SSH key.
7. Click **Yes** to verify the fingerprint and accept the FortiWeb appliance's SSH key. You cannot log in until you accept the key.

   The CLI displays a login prompt.
8. Enter the username you specified in the Azure virtual machine basic settings (**FortiWeb Administrative Username**).
9. For password, enter the password you specified in the basic settings (**FortiWeb Password**).

If 3 incorrect login or password attempts occur in a row, FortiWeb temporarily blacklists your IP address from the GUI and CLI. This action protects the appliance from brute force login attacks. Wait 1 minute, and then attempt the login again.

The CLI displays a prompt, such as:

```
FortiWeb #
```

Uploading the license

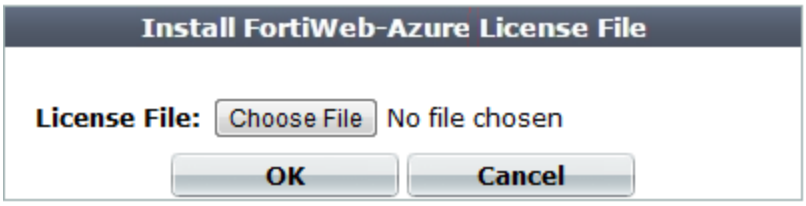
You can upload the FortiWeb-VM license via a web browser connection to the web UI or the CLI. No maintenance period scheduling is required. The uploading process does not interrupt traffic or trigger an appliance reboot.

To upload the license via the web UI

1. Log in to the web UI using the public IP address for your FortiWeb-VM Azure instance. See Connecting to FortiWeb's web UI & CLI on page 17.

   On the status dashboard, the **FortiGuard Information** widget displays the current license status and provides the link you use to upload the license file.

2. By **VM License** , click **Update**.



3. Depending on your browser, either a **Browse** or **Choose File** button is displayed. Locate the license file (.lic) you downloaded earlier from Fortinet, then click **OK**.

   Your browser uploads the license file. Time required varies by the size of the file and the speed of the network connection. If you have uploaded a file that is not a license file, an error message is displayed:

   ```
   Uploaded file is not a license. Please upload a valid license.
   ```

   If you upload the right file type, FortiWeb connects to Fortinet to validate its license. Time required varies, but is usually only a few seconds. A message is displayed:

   ```
   License has been uploaded. Please wait for authentication with registration
       servers.
   ```

4. In the message box, click **Refresh**.

   If you uploaded a valid license, the following message is displayed:

   ```
   License has been successfully authenticated with registration servers.
   ```

   The web UI logs you out. The login dialog reappears.

5. Log in again.

6. To verify that the license was uploaded successfully, log in to the web UI again, then view the **FortiGuard Information** widget. The **VM License** row should say **Valid**.

   Also view the **System Information** widget. The **Serial Number** row displays the maximum number of vCPUs that you can allocate according to the FortiWeb-VM software license, such as **FVVM040000003619** (where "VM04" indicates a limit of 2 vCPUs).

To upload the license via the CLI

1. Using an SSH client, log in to the CLI. See Connecting to FortiWeb's web UI & CLI on page 17.
2. Enter the following command:

```
execute restore vmlicense {ftp | tftp} <license-file_str> {<ftp_ipv4> | <user_
    str>:<password_str>@<ftp_ipv4> | <tftp_ipv4>}
```

   where:

   `{ftp | tftp}` specifies whether to connect to the server using file transfer protocol (FTP) or trivial file transfer protocol (TFTP).

   `<license-file_str>` is the name of the license file.

   `{<ftp_ipv4>` is the IP address of the FTP server.

   `<user_str>` is the user name that FortiWeb uses to authenticate with the server.

   `<password_str>` is the password for the account specified by `<user_str>`.

   `<tftp_ipv4>` is the IP address of the TFTP server.

3. Confirm that you want to perform the license upload.

   After the license is authenticated successfully, the following message is displayed:

```
"*ATTENTION*: license registration status changed to 'VALID', please logout and re-
    login"
```

4. Continue with What's next?.

Integrating with Azure Event Hub

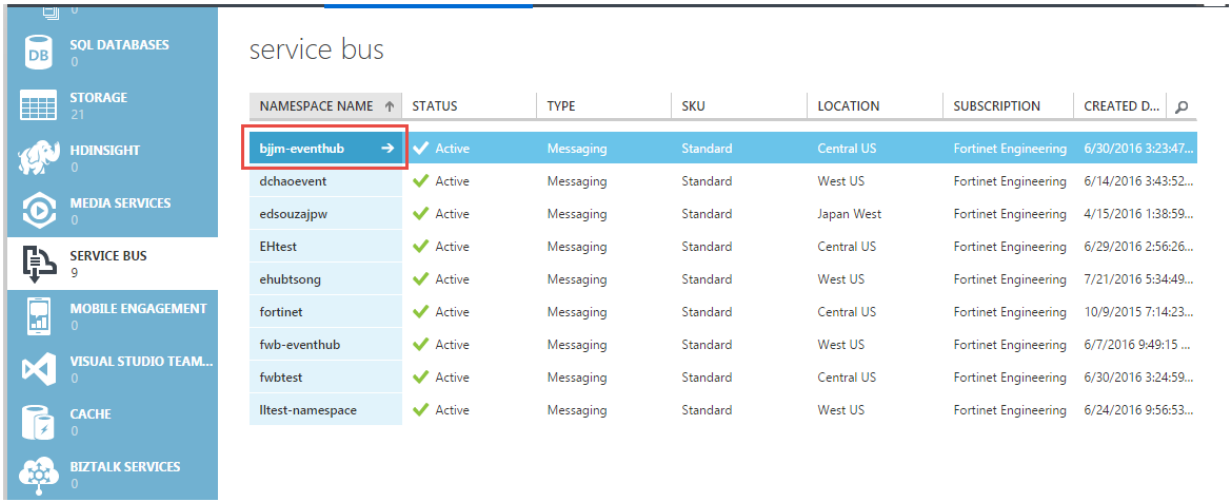
You can integrate FortiWeb-VM with Azure Security Center (ASC) by pushing log messages (event logs, security and health alerts) to an Azure Event Hub. Configuration for the integration starts with connecting the Azure Event Hub to FortiWeb-VM first through either a CLI command or Azure PowerShell. Both the ways will ask you to input necessary information of the event hub you would like to connect to, the asked parameters are:

- **Service Bus Namespace**: The Service Bus Namespace that the Event Hub is created at. This will be required later for parameter `servicebus_namespace`.
- **Name of the Event Hub**: This will be required later for parameter `eventhub_name`.
- **Subscription (ID)**: The subscription (ID) that has the access to the Event Hub. This will be required later for parameter `subscription_id`.
- **Policy name**: Name of the Shared Access policy you created for the Event Hub. This will be required later for parameter `policy_name`.
- **Primary key**: The primary shared access key that the above policy uses for Shared Access Signature authentication on the Event Hub. This will be required later for parameter `primary_key`.

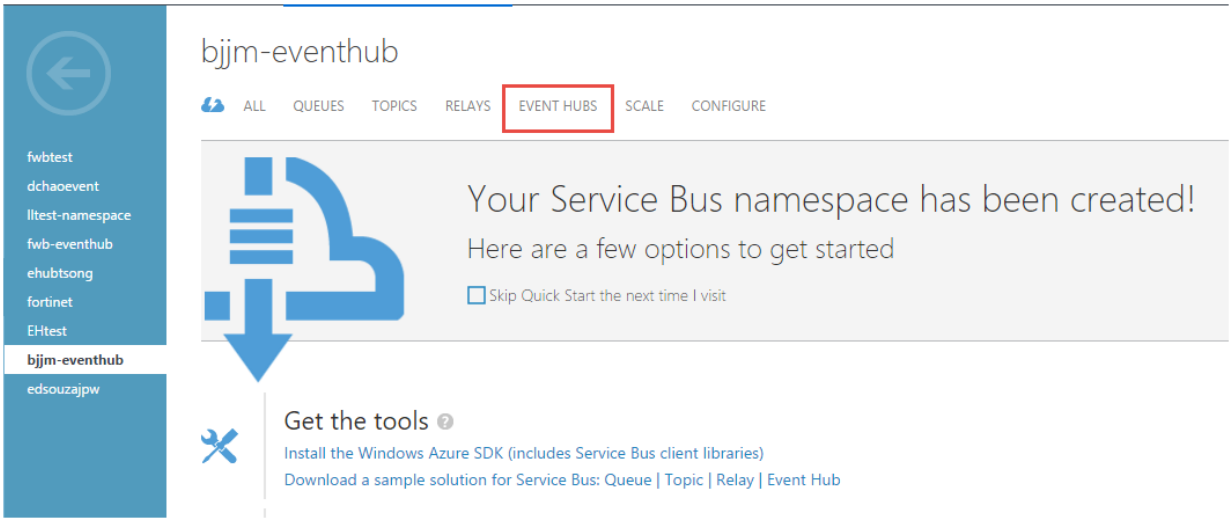
To collect information of an Azure event hub

You can collect the values through the Azure classic portal.

1. To obtain the `servicebus_namespace` value, in the Azure classic portal, In the left navigation pane, click **Service Bus**.
2. Locate the appropriate namespace in the list of namespaces and record its name.

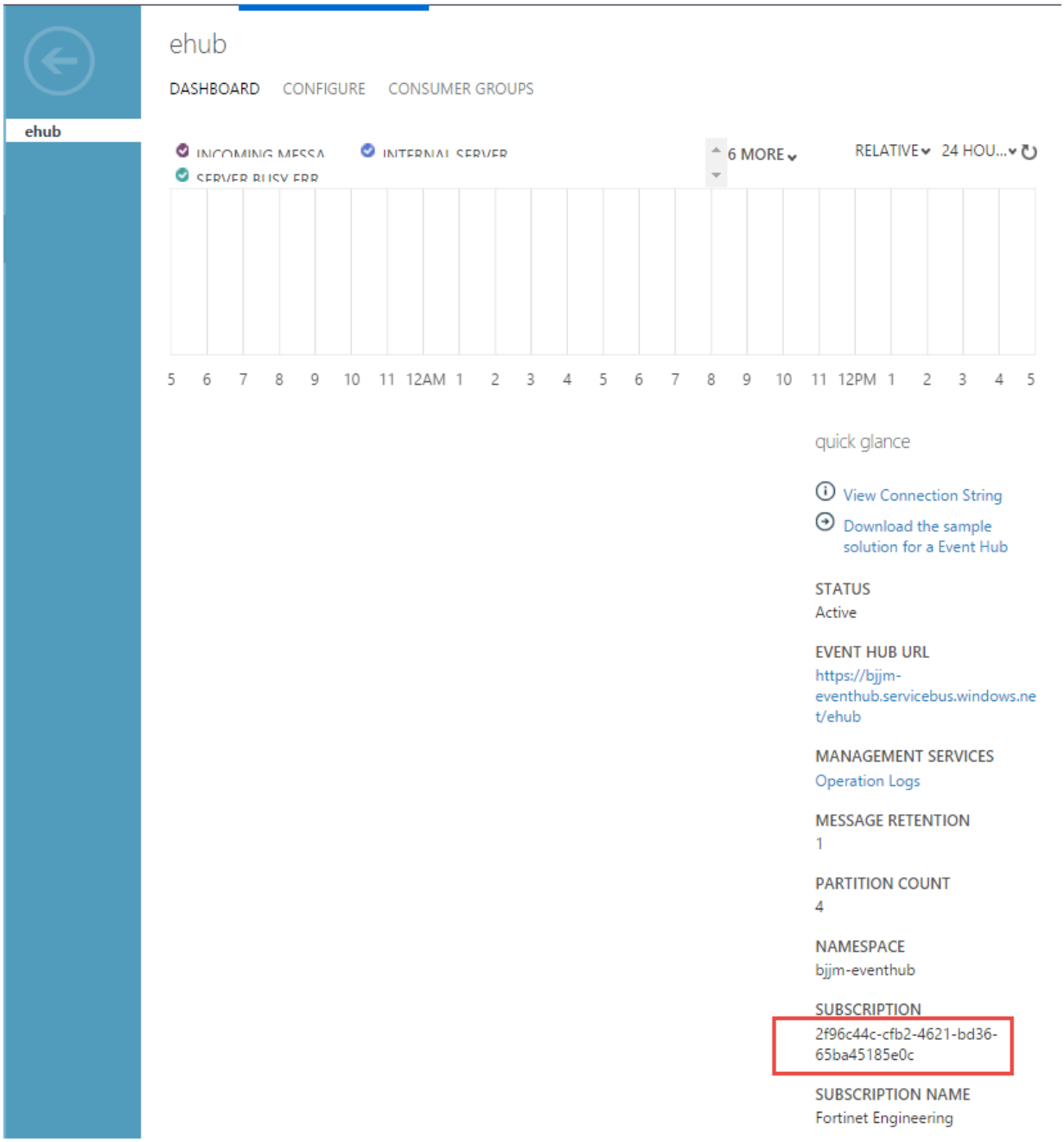


3. To obtain the `eventhub_name` value, click the namespace item you are using, and then click **Event Hubs**.

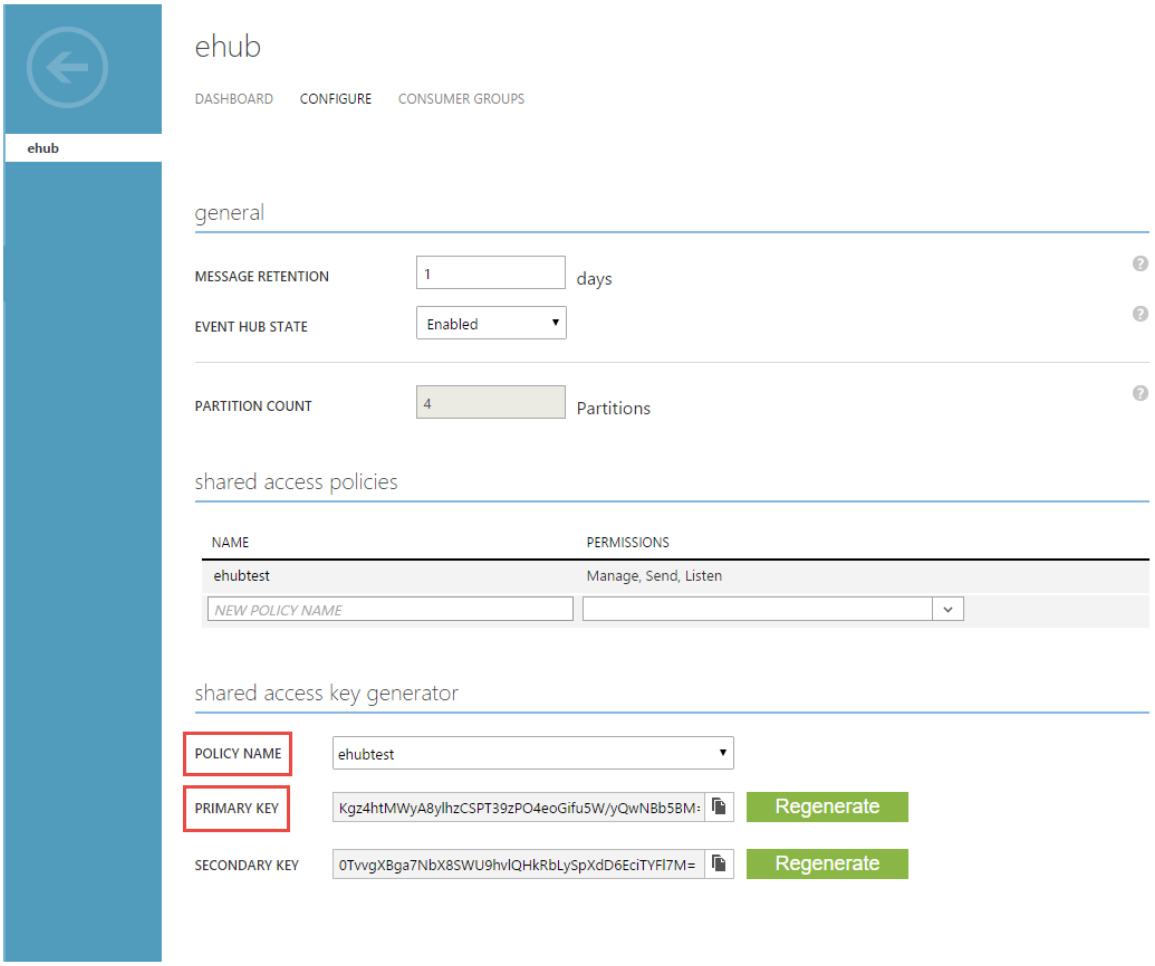


4. Record the event hub name that is displayed.

5. To obtain the `subscription_id` value (displayed in Azure as a Subscription value), first click the name of the event hub you are using to display its properties.
6. Record the Subscription value found in the bottom-right area of the event hub's dashboard. Use this value for `subscription_id`.



7. To access the event hub policy that provides the `policy_name` and `primary_key` values, in the event hub properties, click **Configure**.
8. Record the values **Policy Name** and **Primary Key** values.



So far you have the parameters prepared for connecting the event hub to FortiWeb-VM through the CLI command or Azure PowerShell.

Connect the Azure event hub to FortiWeb-VM through CLI command

Execute the CLI command `system eventhub` with parameters you prepared as following to configure the Azure event hub settings on FortiWeb:

```
config system eventhub
   set status enable
   set appliance_id <subscription_id>
   set policy_saskey <primary_key>
   set policy_name <policy_name>
   set eventhub_name <eventhub_name>
   set servicebus_namespace <servicebus_namespace>
```

For more information on using the CLI, see the *FortiWeb CLI Reference*.

Connect the Azure event hub to FortiWeb-VM through Azure PowerShell

To connect an event hub to FortiWeb-VM through Azure PowerShell, you need to prepare the following files:

A PowerShell script: This is a script (.ps1) that you have to run it through Azure PowerShell to set login information of the Azure event hub into FortiWeb-VM.Contact to Fortinet Technical Support to obtain the script file.

A event hub configuration: This is a .json file containing the necessary information of the event hub. The above PowerShell script will require the .json file to complete configuration of Azure event hub auto-login for FortiWeb-VM. You can edit the following text and save it as a .json file (for example, logging.json) for using:

```
{
    "Logging": {
        "ApplianceID": "<subscription_id>",
        "LoggingLevel": "Alert",
        "Template": "CEF",
        "Connection": {
            "PolicySASKey": "<primary_key>",
            "PolicyName": "<policy_name>",
            "EventHubName": "<eventhub_name>",
            "ServiceBusNamespace": "<servicebus_namespace>"
        }
    }
}
```

, where `<subscription_id>`, `<primary_key>`, `<policy_name>`, `<eventhub_name>` and `<servicebus_namespace>` are the parameters that you have to edit them according to the real practice. Please remain the whole content above unchanged except the parameters, and save the .json file in your local computer.

Login to Azure PowerShell under your local Windows environment, execute the script (for example, customScriptWrapper.ps1) on Azure PowerShell as following to configure the Azure event hub settings to FortiWeb:

```
PS C:\> ./customScriptWrapper.ps1
-loggingPath "<json_path>"
-fileUris @("http://mystorage.blob.core.windows.net/partners/config-eventhub.sh")
-vmname "FWBQAfwbtest1"
-rgname "fortiwebtest1"
-subscriptionId "<subscription_id>"
-scriptToRun "config-eventhub.sh"
```

, where `<json_path>` is the path you save the json file in local computer (for example, C:\Users\username\Desktop\logging.json), and `<subscription_id>` is the subscription (ID) that has the access to the Event Hub. Please do not change the inputs above for parameters `fileUris`, `vmname`, `rgname` and `scriptToRun`.

Besides the configuration for connecting the Event Hub to FortiWeb-VM, you are required to create a SIEM policy and configure the Global Log Settings to push event logs of FortiWeb-VM to the connected Event Hub. See the *FortiWeb Administration Guide*.

What's next?

At this point, the FortiWeb-VM virtual appliance is running, and it has received a license file, but its operating system is almost entirely unconfigured. Before you can use FortiWeb-VM, you must configure it.

Configure the FortiWeb-VM software using the *FortiWeb Administration Guide*.

After you have completed this first-time setup, you can refer to the *FortiWeb Administration Guide* and/or *FortiWeb CLI Reference*. Updates, reconfiguration, and ongoing use of both FortiWeb-VM virtual appliances and physical appliance models such as FortiWeb-3000C are the same.